Elementarteilersatz und Normalformen

Hischer, H.
Kowalsky, H.-J.

Veröffentlicht in:
Abhandlungen der Braunschweigischen
Wissenschaftlichen Gesellschaft Band 28, 1977,
S.69-79

Verlag Erich Goltze KG, Göttingen

Elementarteilersatz und Normalformen

Von **H. Hischer** und **H.-J. Kowalsky**, Braunschweig

Einleitung

Ist A eine n-reihige quadratische Matrix mit Elementen aus einem Körper K, so ist $A-tE$ eine „Polynommatrix" mit Elementen aus K[t]. Nach dem Elementarteilersatz ist sie zu einer Diagonalmatrix

$$S(t) = \begin{pmatrix} f_1(t) & & \\ & \ddots & \\ & & f_n(t) \end{pmatrix}$$

mit Polynomen $f_\nu \in K[t]$ $(\nu = 1,\ldots,n)$ und mit $f_\nu | f_{\nu+1}$ $(\nu = 1,\ldots,n-1)$ äquivalent. Es gibt also invertierbare Polynommatrizen P(t) und Q(t) mit $P(t)(A-tE)Q(t) = S(t)$. Die Matrix S(t) wird auch SMITH'sche Normalform von $A-tE$ genannt. In ihr ist f_n das Minimalpolynom von A, und das Produkt $f_1 \ldots f_n$ ist das charakteristische Polynom von A.

Mit S(t) stehen bekanntlich die zu A ähnlichen Normalmatrizen (JORDAN'sche Normalform usw.) in engem Zusammenhang: Die Polynome $f_1,\ldots,f_n$ gestatten Aussagen über den Zerfall der Normalmatrizen und über den Aufbau ihrer irreduziblen Bestandteile. Sind außerdem die Matrizen P(t) und Q(t) bekannt, so können mit ihrer Hilfe die Ähnlichkeitstransformationen berechnet werden, die A in eine entsprechende Normalform überführen. (Vgl. H. HISCHER, Zur Konstruktion von Normalmatrizen, Braunschweiger Dissertationen 1976.) Hier soll untersucht werden, wie mit Hilfe des Elementarteilersatzes konstruktiv die Existenz von Normalformen bewiesen werden kann und wie die Ergebnisse praktisch genutzt werden können.

1. Vorbemerkungen und Bezeichnungen

Nachfolgend sei K stets ein Körper, X sei ein n-dimensionaler Vektorraum über K, und $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$ sei eine feste Basis von X.

$$\hat{X} = X[t] = K[t] \underset{K}{\otimes} X$$

ist eine Erweiterung von X zu einem K[t]-Modul. Elemente von $\hat{X}$ sind „Polynomvektoren" $\hat{\mathbf{x}}$, die eine eindeutige Darstellung der Form

$$(1) \qquad \hat{\mathbf{x}} = g_1\mathbf{e}_1 + \ldots + g_n\mathbf{e}_n$$

mit Polynomen $g_\nu \in K[t]$ besitzen. Ordnet man rechts nach Potenzen von t, so erhält man eine zweite, ebenfalls eindeutige Darstellung

$$(2) \qquad \hat{\mathbf{x}} = \mathbf{a}_0 + t\mathbf{a}_1 + \ldots + t^r\mathbf{a}_r$$

mit Vektoren $\mathbf{a}_\varrho \in X$ und mit $r = \max\{\text{grad } g_\nu : \nu = 1,\ldots,n\}$.

Ein vom Nullvektor verschiedener Polynomvektor $\hat{\mathbf{x}} \in \hat{X}$ ist genau dann Basisvektor in einer geeigneten Basis von $\hat{X}$, wenn in seiner Darstellung (1) die Polynome $g_1,\ldots,g_n$ teilerfremd sind. Gleichwertig hiermit ist, daß aus $\hat{\mathbf{x}} = g\hat{\mathbf{y}}$ mit $g \in K[t]$ notwendig grad $g = 0$ folgt.

Jedem Modulendomorphismus $\hat{\varphi}: \hat{X} \to \hat{X}$ ist bezüglich der Basis von X eine Polynommatrix $\hat{A} = (g_{\mu,\nu})$ zugeordnet, deren Elemente durch

$$\hat{\varphi}\mathbf{e}_\mu = \sum_{\nu=1}^{n} g_{\mu,\nu}\,\mathbf{e}_\nu \quad (\mu = 1,\ldots,n) \tag{3}$$

bestimmt sind. Außerdem besitzt $\hat{\varphi}$ eine eindeutige Darstellung

$$\hat{\varphi} = \sum_{\sigma=0}^{s} t^\sigma \varphi_\sigma \tag{4}$$

mit Vektorraumendomorphismen $\varphi_\sigma: X \to X$, die umgekehrt zur Definition eines Modulendomorphismus $\hat{\varphi}$ beliebig vorgeschrieben werden können. In diesem Sinn kann speziell jeder Endomorphismus $\varphi: X \to X$ auch als Endomorphismus von $\hat{X}$ aufgefaßt werden. Mit den Bezeichnungen aus (2) und (4) gilt

$$\hat{\varphi}\,\hat{\mathbf{x}} = \sum_{\sigma=0}^{s} \sum_{\varrho=0}^{r} t^{\sigma+\varrho}\,(\varphi_\sigma \mathbf{a}_\varrho).$$

Es sei jetzt f ein festes Polynom aus K[t] mit grad $f = m$. Der kanonische Ringhomomorphismus $\varkappa_f: K[t] \to {}^{K[t]}/_{(f)}$ induziert den Modulhomomorphismus

$$\hat{\varkappa}_f = \varkappa_f \underset{K}{\otimes} \mathrm{id}_X: \hat{X} \to \hat{X}_f$$

auf den $({}^{K[t]}/_{(f)})$-Modul $\hat{X}_f = ({}^{K[t]}/_{(f)}) \otimes X$. Mit den Bezeichnungen aus (1) und (2) gilt

$$\hat{\varkappa}_f\,\hat{\mathbf{x}} = \sum_{\nu=1}^{n} (\varkappa_f g_\nu)\,\mathbf{e}_\nu = \sum_{\varrho=0}^{r} (\varkappa_f t^\varrho)\,\mathbf{a}_\varrho.$$

Nun wird aber jedes Element von ${}^{K[t]}/_{(f)}$ durch ein eindeutig bestimmtes Polynom $h \in K[t]$ mit grad $h < m = \text{grad } f$ bzw. durch das Nullpolynom repräsentiert. In diesem Sinn besitzt jedes $\hat{\mathbf{x}}_f \in \hat{X}_f$ eindeutige Darstellungen

$$\hat{\mathbf{x}}_f = \sum_{\nu=1}^{n} h_\nu \mathbf{e}_\nu = \sum_{\mu=0}^{m-1} t^\mu \mathbf{a}_\mu$$

mit grad $h_\nu \leq m-1$ bzw. $h_\nu = 0$ $(\nu = 1,\ldots,n)$ und mit gewissen $\mathbf{a}_\mu \in X$ $(\mu = 0,\ldots,m-1)$. Schließlich ergibt sich unmittelbar: Zu jedem Endomorphismus $\hat{\varphi}: \hat{X} \to \hat{X}$ gibt es genau einen Endomorphismus $\hat{\varphi}_f: \hat{X}_f \to \hat{X}_f$ mit $\hat{\varphi}_f \circ \hat{\varkappa}_f = \hat{\varkappa}_f \circ \hat{\varphi}$.

2. Induzierte Basen

Die in der Einleitung erwähnte Matrizengleichung kann in der gleichwertigen Form $P(t)(A - tE) = S(t)Q^{-1}(t)$ folgendermaßen gedeutet werden: Durch die Matrix A wird hinsichtlich der Basis $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$ von X ein Endomorphismus $\varphi: X \to X$ beschrieben, durch $A - tE$ also der mit der Identität ε gebildete Modulendomorphismus $\varphi - t\varepsilon: \hat{X} \to \hat{X}$. Die invertierbare Polynommatrix P(t) transformiert die Basis $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$ in eine Basis $\{\hat{\mathbf{b}}_1,\ldots,\hat{\mathbf{b}}_n\}$ von $\hat{X}$, und ebenso gewinnt man mit $Q^{-1}(t)$ eine Basis $\{\hat{\mathbf{c}}_1,\ldots,\hat{\mathbf{c}}_n\}$ von $\hat{X}$. Der Elementarteilersatz kann daher in dem vorliegenden Fall auch so formuliert werden:

Zu jedem Endomorphismus $\varphi: X \to X$ *gibt es Basen* $\{\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n\}$ *und* $\{\hat{\mathbf{c}}_1, \ldots, \hat{\mathbf{c}}_n\}$ *von* $\hat{X}$ *sowie Polynome* $f_1, \ldots, f_n \in K[t]$ *mit*

$$(5) \qquad (\varphi - t\varepsilon)\,\hat{\mathbf{b}}_\nu = f_\nu \hat{\mathbf{c}}_\nu \ (\nu = 1, \ldots, n) \ \textit{und} \ f_\nu | f_{\nu+1} \ (\nu = 1, \ldots, n-1).$$

Gewisse der Vektoren $\hat{\mathbf{b}}_\nu$ sollen nun dazu benutzt werden, um spezielle Basen von X zu konstruieren.

2.1 *Es sei* $\varphi: X \to X$ *ein Endomorphismus, und* $\hat{\mathbf{b}}, \hat{\mathbf{c}}$ *seien Polynomvektoren aus geeigneten Basen von* $\hat{X}$ *mit* $(\varphi - t\varepsilon)\,\hat{\mathbf{b}} = f\hat{\mathbf{c}}$ *und mit* $\operatorname{grad} f = m \geq 1$. *Ferner sei*

$$\hat{\varkappa}_f \hat{\mathbf{b}} = \mathbf{a}_0 + t\mathbf{a}_1 + \ldots + t^{m-1}\mathbf{a}_{m-1}$$

mit geeigneten Vektoren $\mathbf{a}_0, \ldots, \mathbf{a}_{m-1} \in X$. *Dann gilt:*

Die Vektoren $\mathbf{a}_0, \ldots, \mathbf{a}_{m-1}$ *und ebenso die Vektoren* $\mathbf{a}_{m-1}, \varphi\mathbf{a}_{m-1}, \ldots, \varphi^{m-1}\mathbf{a}_{m-1}$ *aus X sind linear unabhängig und erzeugen denselben Unterraum von X. Ferner gilt* $f(\varphi)\mathbf{a}_0 = \ldots = f(\varphi)\mathbf{a}_{m-1} = \mathbf{o}$.

Beweis: Ohne Beschränkung der Allgemeinheit kann f als normiertes Polynom angenommen werden:

$$f(t) = c_0 + c_1 t + \ldots + c_{m-1}t^{m-1} + t^m.$$

Wegen

$$(6) \qquad (\varphi - t\varepsilon)_f \circ \hat{\varkappa}_f \hat{\mathbf{b}} = \hat{\varkappa}_f \circ (\varphi - t\varepsilon)\hat{\mathbf{b}} = \hat{\varkappa}_f(f\hat{\mathbf{c}}) = \hat{\mathbf{o}}_f$$

folgt

$$\begin{aligned} &\varphi\mathbf{a}_0 + t\varphi\mathbf{a}_1 + \ldots + t^{m-1}\varphi\mathbf{a}_{m-1} \\ &\quad = t\mathbf{a}_0 + t^2\mathbf{a}_1 + \ldots + t^{m-1}\mathbf{a}_{m-2} - (c_0 + \ldots + c_{m-1}t^{m-1})\mathbf{a}_{m-1} \end{aligned}$$

und daher

$$(7) \qquad \varphi\mathbf{a}_0 = -c_0\mathbf{a}_{m-1} \ \textit{und} \ \varphi\mathbf{a}_\mu = \mathbf{a}_{\mu-1} - c_\mu\mathbf{a}_{m-1} \ (\mu = 1, \ldots, m-1).$$

Aus diesen Gleichungen ergibt sich mit Hilfe einfacher Umformungen

$$(8) \qquad \begin{aligned} \mathbf{a}_{m-2} &= (\varphi + c_{m-1}\varepsilon)\mathbf{a}_{m-1}, \\ \mathbf{a}_{m-3} &= (\varphi^2 + c_{m-1}\varphi + c_{m-2}\varepsilon)\mathbf{a}_{m-1}, \\ &\vdots \\ \mathbf{a}_1 &= (\varphi^{m-2} + c_{m-1}\varphi^{m-3} + \ldots + c_2\varepsilon)\mathbf{a}_{m-1}, \\ \mathbf{a}_0 &= (\varphi^{m-1} + c_{m-1}\varphi^{m-2} + \ldots + c_1\varepsilon)\mathbf{a}_{m-1}, \end{aligned}$$

und diese Gleichungen können umgekehrt nach $\mathbf{a}_{m-1}, \varphi\mathbf{a}_{m-1}, \ldots, \varphi^{m-1}\mathbf{a}_{m-1}$ aufgelöst werden. Daher erzeugen die Vektoren $\mathbf{a}_0, \ldots, \mathbf{a}_{m-1}$ und $\mathbf{a}_{m-1}, \ldots, \varphi^{m-1}\mathbf{a}_{m-1}$ denselben Unterraum U von X, für den außerdem $\varphi U \subset U$ gilt. Ferner folgt aus der letzten Gleichung (8) und der ersten Gleichung (7)

$$\begin{aligned} f(\varphi)\mathbf{a}_{m-1} &= (\varphi^m + c_{m-1}\varphi^{m-1} + \ldots + c_1\varphi + c_0\varepsilon)\mathbf{a}_{m-1} \\ &= \varphi\mathbf{a}_0 + c_0\mathbf{a}_{m-1} = \mathbf{o} \end{aligned}$$

und daher wieder mit Hilfe von (8) auch $f(\varphi)\mathbf{a}_{m-2} = \ldots = f(\varphi)\mathbf{a}_0 = \mathbf{o}$. Es ist also nur noch die behauptete lineare Unabhängigkeit zu beweisen.

Aus $\mathbf{a}_{m-1} = \mathbf{o}$ würde wegen (8) auch $\mathbf{a}_{m-2} = \ldots = \mathbf{a}_0 = \mathbf{o}$ und daher $\hat{\varkappa}_f \hat{\mathbf{b}} = \hat{\mathbf{o}}_f$, also $\hat{\mathbf{b}} = f\hat{\mathbf{b}}_0$ mit einem geeigneten $\hat{\mathbf{b}}_0$ folgen. Dies widerspricht wegen grad $f \geq 1$ der Voraussetzung, daß $\hat{\mathbf{b}}$ einer Basis von $\hat{X}$ entstammt. Es gilt also $\mathbf{a}_{m-1} \neq \mathbf{o}$.

Es werde nun angenommen, daß die Vektoren $\mathbf{a}_0, \ldots, \mathbf{a}_{m-1}$ linear abhängig sind. Mit $\mathbf{a}_0$ beginnend drücke man dann abhängige Vektoren als Linearkombination folgender Vektoren aus. Der erste nicht so darstellbare Vektor werde mit $\mathbf{b}_1$ bezeichnet, der nächste nicht so darstellbare Vektor mit $\mathbf{b}_2$ usw. Man erhält

$$\hat{\varkappa}_f \hat{\mathbf{b}} = g_1 \mathbf{b}_1 + \ldots + g_r \mathbf{b}_r \tag{9}$$

mit linear unabhängigen Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_r \in X$, mit $r \leq m-1$, mit normierten Polynomen $g_1, \ldots, g_r \in K[t]$ und mit

$$0 \leq \operatorname{grad} g_1 < \operatorname{grad} g_2 < \ldots < \operatorname{grad} g_r = m-1, \tag{10}$$

wobei sich das letzte Gleichheitszeichen wegen $\mathbf{a}_{m-1} \neq \mathbf{o}$ ergibt.

Die Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_r$ bilden eine Basis des φ-invarianten Unterraums U, hinsichtlich derer der Restriktion φ_U eine Matrix $B = (b_{\varrho,\sigma})$ mit Elementen $b_{\varrho,\sigma} \in K$ zugeordnet ist. Wegen (6) und (8) folgt

$$\begin{aligned}
(b_{1,1}-t)g_1(t) + \ldots + b_{1,r-1}g_{r-1}(t) + b_{1,r}g_r(t) &= f(t)h_1(t),\\
b_{r-1,1}g_1(t) + \ldots + (b_{r-1,r-1}-t)g_{r-1}(t) + b_{r-1,r}g_r(t) &= f(t)h_{r-1}(t),\\
b_{r,1}g_1(t) + \ldots + b_{r,r-1}g_{r-1}(t) + (b_{r,r}-t)g_r(t) &= f(t)h_r(t).
\end{aligned} \tag{11}$$

Hier stehen in den ersten r-1 Gleichungen auf den linken Seiten wegen (10) nur Polynome höchstens (m-1)-ten Grades. Wegen grad $f = m$ folgt daher $h_1 = \ldots = h_{r-1} = 0$. Lediglich in der letzten Gleichung liefert eine entsprechende Überlegung bei Berücksichtigung der Normierung $h_r = -1$.

Es soll nun für $\varrho = 1, \ldots, r$

$$g_1 \mid g_\sigma \ (\sigma = 1, \ldots, \varrho) \ \textit{und} \ \operatorname{grad} g_\varrho = (\varrho-1) + \operatorname{grad} g_1 \tag{12}$$

bewiesen werden. Für $\varrho = 1$ ist die Behauptung trivial. Ist (12) für ein ϱ mit $\varrho < r$ erfüllt, so folgt wegen (10)

$$\operatorname{grad} g_1 < \ldots < \operatorname{grad}(b_{\varrho,\varrho}-t)g_\varrho \leq \operatorname{grad} g_{\varrho+1} < \ldots < \operatorname{grad} g_r.$$

In der ϱ-ten Gleichung aus (11) gilt wegen $\varrho < r$ und $h_\varrho = 0$ daher $0 = b_{\varrho,r} = b_{\varrho,r-1} = \ldots = b_{\varrho,\varrho+2}$, so daß sich diese auf

$$b_{\varrho,1}g_1 + \ldots + (b_{\varrho,\varrho}-t)g_\varrho + b_{\varrho,\varrho+1}g_{\varrho+1} = 0$$

reduziert. Es folgt $b_{\varrho,\varrho+1} \neq 0$, wegen (12) dann $g_1 \mid g_{\varrho+1}$ und weiter

$$\operatorname{grad} g_{\varrho+1} = \operatorname{grad}(b_{\varrho,\varrho}-t)g_\varrho = 1 + \operatorname{grad} g_\varrho = \varrho + \operatorname{grad} g_1.$$

Speziell im Fall $\varrho = r$ liefert (12) zusammen mit der letzten Gleichung von (11)

$$\operatorname{grad} g_1 = \operatorname{grad} g_r - (r-1) = m - r \geq 1.$$

Der erste Teil von (12) ergibt wegen (9) wieder $\hat{\varkappa}_f \hat{\mathbf{b}} = g_1 \hat{\mathbf{b}}_0$ mit einem geeigneten $\hat{\mathbf{b}}_0$, also wegen grad $g_1 \geq 1$ denselben Widerspruch wie oben. Damit ist auch die lineare Unabhängigkeit der Vektoren $\mathbf{a}_0, \ldots, \mathbf{a}_{m-1}$ und der Vektoren $\mathbf{a}_{m-1}, \ldots, \varphi^{m-1}\mathbf{a}_{m-1}$ bewiesen. ■

Wesentlich einfacher ergibt sich die folgende Umkehrung von 2.1.

2.2 *Es sei* $\varphi: X \to X$ *ein Endomorphismus, und die Vektoren* $\mathbf{a}, \varphi\mathbf{a}, \ldots, \varphi^{m-1}\mathbf{a}$ $(m \geq 1)$ *seien linear unabhängig. Ferner sei* $f(\varphi)\mathbf{a} = \mathbf{o}$ *mit dem Polynom* $f(t) = c_0 + \ldots + c_{m-1}t^{m-1} + t^m$ *erfüllt. Setzt man dann* $\mathbf{a}_{m-1} = \mathbf{a}$ *und definiert man die Vektoren* $\mathbf{a}_{m-2}, \ldots, \mathbf{a}_0$ *durch die Gleichungen* (8), *so gibt es zu*

$$\hat{\mathbf{b}} = \mathbf{a}_0 + t\mathbf{a}_1 + \ldots + t^{m-1}\mathbf{a}_{m-1}$$

einen Vektor $\hat{\mathbf{c}}$ *mit* $(\varphi - t\varepsilon)\hat{\mathbf{b}} = f\hat{\mathbf{c}}$.

Beweis: Aus den Gleichungen (8) folgen wegen $f(\varphi)\mathbf{a}_{m-1} = \mathbf{o}$ umgekehrt die Gleichungen (7), mit deren Hilfe man

$$\varphi\hat{\mathbf{b}} = t\mathbf{a}_0 + \ldots + t^{m-1}\mathbf{a}_{m-2} - (c_0 + \ldots + c_{m-1}t^{m-1})\mathbf{a}_{m-1}$$

erhält und weiter

$$(\varphi - t\varepsilon)\hat{\mathbf{b}} = -(c_0 + \ldots + c_{m-1}t^{m-1} + t^m)\mathbf{a}_{m-1} = -f(t)\mathbf{a}_{m-1}. \blacksquare$$

Aus den beiden bisher bewiesenen Sätzen sollen nun einige Folgerungen gezogen werden. Unter den in den Gleichungen (5) auftretenden Polynomen können einige konstant sein. Es soll daher weiter

(13) $\quad \operatorname{grad} f_1 = \ldots = \operatorname{grad} f_{q-1} = 0$ *und* $\operatorname{grad} f_\nu \geq 1$ *für* $\nu \geq q$ $(q \geq 1)$

vorausgesetzt werden, wobei dann

(14) $\quad \operatorname{grad} f_q + \ldots + \operatorname{grad} f_n = n$

erfüllt ist. Wendet man nun 2.1 auf die Basisvektoren $\hat{\mathbf{b}}_\nu, \hat{\mathbf{c}}_\nu$ und die Polynome f_ν $(\nu \geq q)$ an, so folgt

$$\hat{\varkappa}_{f_\nu}\hat{\mathbf{b}}_\nu = \mathbf{a}_{\nu,0} + t\mathbf{a}_{\nu,1} + \ldots + t^{m_\nu - 1}\mathbf{a}_{\nu, m_\nu - 1}$$

mit linear unabhängigen Vektoren $\mathbf{a}_{\nu,0}, \ldots, \mathbf{a}_{\nu, m_\nu - 1}$ und mit $m_\nu = \operatorname{grad} f_\nu$. Gezeigt werden soll, daß diese Vektoren nicht nur bei festem ν, sondern insgesamt linear unabhängig sind und somit eine Basis von X bilden.

Ist $\mathbf{a} \neq \mathbf{o}$ ein Vektor aus X, so sind jedenfalls die $n+1$ Vektoren $\mathbf{a}, \varphi\mathbf{a}, \ldots, \varphi^n\mathbf{a}$ linear abhängig. Es gibt daher ein normiertes Polynom $f_\mathbf{a}$ kleinsten Grades mit $f_\mathbf{a}(\varphi)\,\mathbf{a} = \mathbf{o}$. Anwendung von 2.2 ergibt $(\varphi - t\varepsilon)\,\hat{\mathbf{b}} = f_\mathbf{a}\hat{\mathbf{c}}$ mit dem entsprechend gebildeten Vektor $\hat{\mathbf{b}}$, der sich als Linearkombination

$$\hat{\mathbf{b}} = g_1\hat{\mathbf{b}}_1 + \ldots + g_n\hat{\mathbf{b}}_n \quad \textit{mit } g_1, \ldots, g_n \in K[t]$$

darstellen lassen muß. Es folgt

$$(\varphi - t\varepsilon)\,\hat{\mathbf{b}} = g_1 f_1\hat{\mathbf{c}}_1 + \ldots + g_n f_n\hat{\mathbf{c}}_n = f_\mathbf{a}\hat{\mathbf{c}},$$

und wegen (13) müssen daher jedenfalls die Polynome $g_1, \ldots, g_{q-1}$ durch $f_\mathbf{a}$ teilbar sein. Da aber $\hat{\mathbf{b}} = \hat{\varkappa}_{f_\mathbf{a}}\hat{\mathbf{b}}$ gilt, muß $\hat{\mathbf{b}}$ sogar als Linearkombination von $\hat{\mathbf{b}}_q, \ldots, \hat{\mathbf{b}}_n$ modulo $f_\mathbf{a}$ darstellbar sein. Da aber $\hat{\mathbf{b}}$ umgekehrt $\mathbf{a}$ bestimmt, ist $\mathbf{a}$ als Linearkombination der Menge $\mathbf{B} = \{\mathbf{a}_{\nu,\mu} : \nu = q, \ldots, n,\ \mu = 0, \ldots, m_\nu - 1\}$ darstellbar. Und da schließlich $\mathbf{a} \in X$ beliebig gewählt war, erzeugt $\mathbf{B}$ den ganzen Vektorraum X. Weil $\mathbf{B}$ aber wegen (14) aus genau n Vektoren besteht, gilt sogar

2.3 $\mathbf{B} = \{\mathbf{a}_{\nu,\mu} : \nu = q,\ldots,n,\ \mu = 0,\ldots,m_\nu\text{-}1\}$ *ist eine Basis von* X.

Der folgende Satz dient nun noch einer Modifikation dieser Basis, die dem Zerfall der Polynome f_ν in teilerfremde Faktoren entspricht.

2.4 *Es sei* $f = f_1 \cdot f_2$ *mit* $(f_1, f_2) = 1$, grad $f_1 = r$, grad $f_2 = s$ *und* grad $f = m = r+s$. *Ferner gelte mit linear unabhängigen Vektoren* $\mathbf{a}_0,\ldots,\mathbf{a}_{m-1} \in X$

$$\hat{\varkappa}_{f_1}(\mathbf{a}_0 + t\mathbf{a}_1 + \ldots + t^{m-1}\mathbf{a}_{m-1}) = \mathbf{b}_0 + t\mathbf{b}_1 + \ldots + t^{r-1}\mathbf{b}_{r-1},$$
$$\hat{\varkappa}_{f_2}(\mathbf{a}_0 + t\mathbf{a}_1 + \ldots + t^{m-1}\mathbf{a}_{m-1}) = \mathbf{c}_0 + t\mathbf{c}_1 + \ldots + t^{s-1}\mathbf{c}_{s-1}.$$

Dann sind die Vektoren $\mathbf{b}_0,\ldots,\mathbf{b}_{r-1}, \mathbf{c}_0,\ldots,\mathbf{c}_{s-1}$ *aus* X *ebenfalls linear unabhängig und spannen denselben Unterraum wie die Vektoren* $\mathbf{a}_0,\ldots,\mathbf{a}_{m-1}$ *auf.*

Beweis: Mit geeigneten Skalaren gilt

$$\mathbf{b}_\varrho = \sum_{\mu=0}^{m-1} b_{\varrho,\mu}\,\mathbf{a}_\mu \ (\varrho = 0,\ldots,r\text{-}1), \quad \mathbf{c}_\sigma = \sum_{\mu=0}^{m-1} c_{\sigma,\mu}\,\mathbf{a}_\mu \ (\sigma = 0,\ldots,s\text{-}1).$$

Der von diesen Vektoren aufgespannte Unterraum ist also jedenfalls in dem von den Vektoren $\mathbf{a}_0,\ldots,\mathbf{a}_{m-1}$ erzeugten Unterraum enthalten, so daß nur noch die behauptete lineare Unabhängigkeit nachgewiesen werden muß. Wegen

$$\hat{\varkappa}_{f_1}\Big(\sum_{\mu=0}^{m-1} t^\mu \mathbf{a}_\mu\Big) = \sum_{\varrho=0}^{r-1} t^\varrho \mathbf{b}_\varrho = \sum_{\mu=0}^{m-1}\sum_{\varrho=0}^{r-1} t^\varrho b_{\varrho,\mu}\,\mathbf{a}_\mu$$

und wegen der linearen Unabhängigkeit der Vektoren $\mathbf{a}_0,\ldots,\mathbf{a}_{m-1}$ ergibt sich

$$\varkappa_{f_1}(t^\mu) = \sum_{\varrho=0}^{r-1} t^\varrho b_{\varrho,\mu} \ (\mu = 0,\ldots,m\text{-}1)$$

und ebenso

$$\varkappa_{f_2}(t^\mu) = \sum_{\sigma=0}^{s-1} t^\sigma c_{\sigma,\mu} \ (\mu = 0,\ldots,m\text{-}1).$$

Nimmt man an, daß die Vektoren $\mathbf{b}_0,\ldots,\mathbf{b}_{r-1}, \mathbf{c}_0,\ldots,\mathbf{c}_{s-1}$ linear abhängig sind, so sind in der Matrix

$$\begin{pmatrix} b_{0,0} & \ldots & b_{0,m-1} \\ \ldots & \ldots & \ldots \\ b_{r-1,0} & \ldots & b_{r-1,m-1} \\ c_{0,0} & \ldots & c_{0,m-1} \\ \ldots & \ldots & \ldots \\ c_{s-1,0} & \ldots & c_{s-1,m-1} \end{pmatrix}$$

die Zeilen und daher auch die Spalten linear abhängig. Es existieren also nicht sämtlich verschwindende Skalare $a_0,\ldots,a_{m-1}$ mit

$$\sum_{\mu=0}^{m-1} b_{\varrho,\mu}\,a_\mu = \sum_{\mu=0}^{m-1} c_{\sigma,\mu}\,a_\mu = 0 \ \textit{für}\ \varrho = 0,\ldots,r\text{-}1,\ \sigma = 0,\ldots,s\text{-}1,$$

und für das durch

$$g(t) = a_0 + a_1 t + \ldots + a_{m-1}t^{m-1}$$

definierte Polynom gilt $g \not\equiv 0$. Es folgt

$$0 = \sum_{\varrho=0}^{r-1} t^\varrho \Big(\sum_{\mu=0}^{m-1} b_{\varrho,\mu}\,a_\mu\Big) = \sum_{\mu=0}^{m-1}\Big(\sum_{\varrho=0}^{r-1} t^\varrho b_{\varrho,\mu}\Big)a_\mu = \varkappa_{f_1}\Big(\sum_{\mu=0}^{m-1} t^\mu a_\mu\Big) = \varkappa_{f_1}(g),$$
$$0 = \sum_{\sigma=0}^{s-1} t^\sigma \Big(\sum_{\mu=0}^{m-1} c_{\sigma,\mu}\,a_\mu\Big) = \sum_{\mu=0}^{m-1}\Big(\sum_{\sigma=0}^{s-1} t^\sigma c_{\sigma,\mu}\Big)a_\mu = \varkappa_{f_2}\Big(\sum_{\mu=0}^{m-1} t^\mu a_\mu\Big) = \varkappa_{f_2}(g),$$

also $f_1 | g$ und $f_2 | g$. Wegen $(f_1, f_2) = 1$ gilt dann aber sogar $f | g$ im Widerspruch zu grad $f = m > m-1 \geq$ grad g. ■

3. Normalmatrizen

Wie in 2.1 sei wieder $\varphi : X \to X$ ein Endomorphismus,

$$f(t) = c_0 + c_1 t + \ldots + c_{m-1} t^{m-1} + t^m$$

sei ein Polynom aus $K[t]$ mit $m \geq 1$, und $\hat{\mathbf{b}}, \hat{\mathbf{c}}$ seien Polynomvektoren aus geeigneten Basen von $\hat{X}$ mit $(\varphi - t\varepsilon)\,\hat{\mathbf{b}} = f\hat{\mathbf{c}}$. Reduziert man dann $\hat{\mathbf{b}}$ modulo f, bildet man also

$$\hat{\varkappa}_f \hat{\mathbf{b}} = \mathbf{a}_0 + t\mathbf{a}_1 + \ldots + t^{m-1}\mathbf{a}_{m-1},$$

so besagte Satz 2.1, daß $\{\mathbf{a}_0, \ldots, \mathbf{a}_{m-1}\}$ eine Basis eines φ-invarianten Unterraums U ist. Der Restriktion φ_U von φ auf diesen Unterraum ist hinsichtlich der Basis $\{\mathbf{a}_0, \ldots, \mathbf{a}_{m-1}\}$ eine Matrix B zugeordnet, deren Elemente sich unmittelbar aus den Gleichungen (7) ergeben und die auch als die „zu f gehörende Begleitmatrix" bezeichnet wird:

$$B = \begin{pmatrix} 0 & \cdots & 0 & -c_0 \\ 1 & \ddots & \vdots & \vdots \\ 0 & \ddots & 0 & -c_{m-2} \\ 0 & \cdots & 1 & -c_{m-1} \end{pmatrix}$$

Sind in (5) wieder die Polynome $f_1, \ldots, f_{q-1}$ konstant, während $f_q, \ldots, f_n$ positiven Grad besitzen, so sind diesen Polynomen $f_q, \ldots, f_n$ und den zugehörigen Basisvektoren $\hat{\mathbf{b}}_q, \ldots, \hat{\mathbf{b}}_n$ also φ-invariante Unterräume $U_q, \ldots, U_n$ zugeordnet, und die entsprechenden Restriktionen von φ werden durch Begleitmatrizen $B_q, \ldots, B_n$ beschrieben. Wegen 2.3 ist aber der Gesamtraum X gerade die direkte Summe der Unterräume $U_q, \ldots, U_n$, und hinsichtlich der Gesamtbasis **B** aus 2.3 entspricht φ die Matrix

$$\begin{pmatrix} \boxed{B_q} & & \\ & \ddots & \\ & & \boxed{B_n} \end{pmatrix}$$

Hier können aber die Blöcke $B_q, \ldots, B_n$ unter Umständen mit Hilfe von 2.4 weiter zerlegt werden. Zur Vereinfachung der Bezeichnung soll hierbei auf den Index verzichtet werden: Es sei also wieder B eine dieser Begleitmatrizen, die wie oben zu dem Polynomvektor $\hat{\mathbf{b}}$ und dem Polynom f gehöre. Stellt man nun f als Produkt von Potenzen verschiedener (über K) irreduzibler Polynome dar,

$$f = p_1^{r_1} \ldots p_s^{r_s},$$

so zerfällt B wegen 2.4 in Blöcke, die aus den zu den Polynomen $p_\sigma^{r_\sigma}$ gehörenden Begleitmatrizen bestehen. Man hat hierzu lediglich $\hat{\mathbf{b}}$ nicht modulo f, sondern jeweils modulo $p_\sigma^{r_\sigma}$ zu betrachten, hat sich also mit $g_\sigma = p_\sigma^{r_\sigma}$ und grad $g_\sigma = m_\sigma$ die Darstellung

$$\hat{\varkappa}_{g_\sigma} \hat{\mathbf{b}} = \mathbf{a}_{\sigma,0} + t\,\mathbf{a}_{\sigma,1} + \ldots + t^{m_\sigma - 1}\mathbf{a}_{\sigma,m_\sigma-1}$$

zu verschaffen, um in den Vektoren $\mathbf{a}_{\sigma,0},\ldots,\mathbf{a}_{\sigma,m_\sigma-1}$ die zu der entsprechenden Begleitmatrix gehörende Basis zu gewinnen.

Aber auch die zu der Potenz p^r eines irreduziblen Polynoms p gehörende Begleitmatrix kann im Fall $r > 1$ noch weiter unterteilt werden. Hierzu sei

und
$$p(t) = a_0 + a_1 t + \ldots + a_{k-1} t^{k-1} + t^k,$$
$$\hat{\mathbf{b}} = \mathbf{b}_0 + t\,\mathbf{b}_1 + \ldots + t^{rk-1}\mathbf{b}_{rk-1}$$

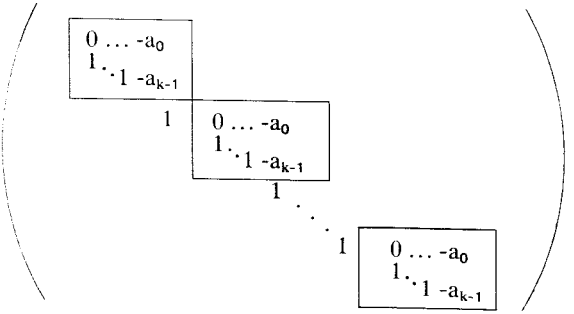
sei jetzt der bereits modulo p^r reduzierte zugehörige Polynomvektor. Die Vektoren $\mathbf{b}_0,\ldots,\mathbf{b}_{rk-1}$ bilden also eine Basis eines φ-invarianten Unterraums, und der Restriktion φ_U entspricht hinsichtlich dieser Basis die zu p^r gehörende Begleitmatrix. Bildet man nun, ähnlich wie in (8), die neuen Vektoren

$$\begin{aligned}
\mathbf{c}_{rk-1} &= \mathbf{b}_{rk-1}\\
\mathbf{c}_{rk-2} &= \varphi\,\mathbf{c}_{rk-1} + a_{k-1}\,\mathbf{b}_{rk-1}\\
&\vdots\\
\mathbf{c}_{(r-1)k-1} &= \varphi\,\mathbf{c}_{rk-k} + a_0\,\mathbf{b}_{rk-1},
\end{aligned}$$

so folgt

$$\mathbf{c}_{(r-1)k-1} = (\varphi^k + a_{k-1}\varphi^{k-1} + \ldots + a_1\varphi + a_0\varepsilon)\,\mathbf{b}_{rk-1}.$$

Daher ist $\mathbf{c}_{(r-1)k-1}$ der Koeffizient von t^{rk-1} bei $\hat{\varkappa}_{p^r}(p(t)\hat{\mathbf{b}})$ oder gleichwertig der Koeffizient von $t^{(r-1)k-1}$ bei $\hat{\varkappa}_{p^{r-1}}\hat{\mathbf{b}}$. Man befindet sich also wieder in der Ausgangssituation, jedoch nur noch hinsichtlich der Potenz p^{r-1}. Man kann daher die Konstruktion mit $\mathbf{c}_{(r-1)k-1}$ statt $\mathbf{b}_{rk-1}$ wiederholen und so sukzessiv den Exponenten von p abbauen. Hinsichtlich der so gewonnenen Basis $\mathbf{c}_0,\ldots,\mathbf{c}_{rk-1}$ des Unterraums ist der Restriktion von φ dann die Matrix



zugeordnet.

4. Praktische Durchführung

Im konkreten Fall ist der Endomorphismus $\varphi: X \to X$ hinsichtlich der Basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ durch eine quadratische Matrix A mit Elementen aus K gegeben. Zu bestimmen sind zunächst invertierbare Polynommatrizen P(t) und Q(t) mit $P(t)(A\text{-}tE)Q(t) = S(t)$. Dabei können P(t) und Q(t) sukzessiv als Produkte von Matrizen gewonnen werden, die elementare Umformungen von A-tE beschreiben; und zwar gehören zu P(t) die Zeilen- und zu Q(t) die Spaltenumformungen. Praktisch geht man so vor, daß man links und rechts neben die Matrix A-tE jeweils die Einheitsmatrix schreibt. Alle an A-tE vorgenommenen Zeilenumformungen sind dann gleichzeitig an der linken Matrix durchzuführen und entsprechend alle Spaltenumformungen an der rechten Matrix. Am Schluß der Umformungen steht dann in der Mitte die Matrix S(t), links P(t) und rechts Q(t).

Zu diesem Verfahren sind einige Bemerkungen zu machen, die sich auf den bei größeren Matrizen recht erheblichen Rechenaufwand beziehen. Erstens ist festzustellen, daß dieser Aufwand in den wesentlichen Teilen ohnehin nicht vermeidbar ist. Denn auch die sonst üblichen Verfahren erfordern die Berechnung des charakteristischen Polynoms, das man meist am einfachsten gewinnt, wenn man A-tE mit Hilfe elementarer Umformungen in eine Dreiecksmatrix überführt. Gerade hierin bestehen aber die aufwendigen Umformungsschritte. Die Erzeugung von Nullen auch auf der anderen Seite der Hauptdiagonalen beinhaltet eine nur unwesentliche Zusatzarbeit. Nachträglich ergeben sich dann aber ganz erhebliche Vereinfachungen. Zweitens braucht man für die weiteren Schritte nur die Polynomvektoren $\hat{\mathbf{b}}_\nu$ aus (5), deren Koordinaten hinsichtlich der Basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ gerade die Zeilen der Matrix P(t) bilden; und zwar braucht man nur diejenigen Zeilen, denen in der Matrix S(t) nichtkonstante Polynome entsprechen. Man kann somit auf die Berechnung der Matrix Q(t) verzichten, braucht also die Umformungen an der rechten Einheitsmatrix nicht durchzuführen. Gerade aus diesem Grund wird man aber nach Möglichkeit Spaltenumformungen bevorzugen. Da nämlich die Matrizen P(t) und Q(t) keineswegs eindeutig sind, kann man auf diese Weise die Matrix P(t) möglichst einfach gestalten.

Sind P(t) und S(t) berechnet, so hat man nur noch die nicht-konstanten Polynome f_ν aus S(t) in Potenzen irreduzibler Polynome zu zerlegen und die entsprechenden Zeilen von P(t) modulo der so gewonnenen Faktoren zu reduzieren. Die dann bei den einzelnen Potenzen von t auftretenden Koeffizientenvektoren bilden insgesamt eine Basis von X, und ihre Koordinaten sind die Zeilen einer Transformationsmatrix T, mit der TAT^{-1} die gesuchte Normalmatrix ist. Zur Erläuterung diene als einfaches Beispiel die Matrix

$$A = \begin{pmatrix} 2 & -4 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 3 & 0 & -2 & 3 \\ 1 & 2 & -1 & 2 \end{pmatrix}$$

Geeignete Umformungen führen hier auf die Matrizen

$$P(t) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & \frac{3}{2}(t-3) & 1 & \frac{3}{2}(1-t) \\ 1 & \frac{1}{2}(-t^2+3t-2) & -1 & \frac{1}{2}(t^2-t+4) \end{pmatrix}$$

und

$$S(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1-t & 0 \\ 0 & 0 & 0 & f(t) \end{pmatrix}$$

mit $f(t) = \frac{1}{2}(1-t)(t^2-t+2)$.

In der SMITH'schen Matrix S(t) ist hier die Faktorzerlegung bezüglich $\mathbb{Q}$ oder $\mathbb{R}$ als Skalarenkörper bereits durchgeführt. Die dritte Zeile von P(t) ist nur modulo 1-t zu reduzieren (es ist also $t = 1$ zu setzen) und ergibt den (Eigen-) Vektor

$$\mathbf{a}_1 = (0, -3, 1, 0).$$

Entsprechend liefert die vierte Zeile von P(t) modulo 1-t den Vektor

$$\mathbf{a}_2 = (1, 0, -1, 2).$$

Hingegen führt Reduktion der vierten Zeile modulo t^2-t+2 auf den Polynomvektor

$$\mathbf{a}_3 + t\mathbf{a}_4 = (1, t, -1, 1) = (1, 0, -1, 1) + t(0, 1, 0, 0,).$$

Mit der durch diese Vektoren $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4$ gebildeten Transformationsmatrix

$$T = \begin{pmatrix} 0 & -3 & 1 & 0 \\ 1 & 0 & -1 & 2 \\ 1 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

gilt dann

$$TAT^{-1} = \begin{pmatrix} \boxed{1} & 0 & 0 & 0 \\ 0 & \boxed{1} & 0 & 0 \\ 0 & 0 & \boxed{0} & \boxed{-2} \\ 0 & 0 & \boxed{1} & \boxed{1} \end{pmatrix}$$

Die konstruktive Umformung der zu Potenzen irreduzibler Polynome gehörenden Untermatrizen wurde bereits im vorangehenden Abschnitt behandelt. Sie soll hier abschließend noch an der Matrix

$$A = \begin{pmatrix} 1 & -1 & -1 & 0 \\ 1 & 12 & 0 & 13 \\ 0 & -9 & 0 & -10 \\ -1 & -8 & 1 & -9 \end{pmatrix}$$

erläutert werden. Entsprechende Umformungen ergeben die Matrizen

$$P(t) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & t & 1 & t \\ 1 & t^3+t & t^2 & t^3+1 \end{pmatrix} \quad \text{und}$$

$$S(t) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -(f(t))^2 \end{pmatrix} \quad \textit{mit } f(t) = t^2-2t+3.$$

Mit den Bezeichnungen aus dem vorangehenden Abschnitt folgt hier

$$\hat{\mathbf{b}} = (1,0,0,1) + t(0,1,0,0) + t^2(0,0,1,0) + t^3(0,1,0,1),$$
$$\mathbf{c}_3 = (0,1,0,1),$$
$$\mathbf{c}_2 = (0,1,0,1)A - 2(0,1,0,1) = (0,2,1,2),$$
$$\mathbf{c}_1 = (0,2,1,2)A + 3(0,1,0,1) = (0,2,2,1),$$
$$\mathbf{c}_0 = (0,2,2,1)A - 2(0,2,2,1) = (1,-6,-3,-5).$$

Hinsichtlich der Basis $\{\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$ entspricht dann dem Endomorphismus die Normalmatrix

$$\begin{pmatrix} 0 & -3 & & \\ 1 & 2 & & \\ & & 0 & -3 \\ & & 1 & 2 \end{pmatrix}$$